Configuring the Cisco VPN 3000 Concentrator for Blocking with Filters and RADIUS Filter Assignment

Document ID: 13834

Introduction

In this sample configuration, we want to use filters to allow a user to access only one server (10.1.1.2) inside the network and block access to all other resources. The Cisco VPN 3000 Concentrator can be set up to control IPsec, Point−to−Point Tunneling Protocol (PPTP), and L2TP client access to network resources with filters. Filters consist of rules, which are similar to access lists on a router. If a router was configured for:

```
access−list 101 permit ip any host 10.1.1.2
access−list 101 deny ip any any
```

the VPN Concentrator equivalent would be to set up a filter with rules.

Our first VPN Concentrator rule is **permit_server_rule**, which is equivalent to the router's **permit ip any host 10.1.1.2** command. Our second VPN Concentrator rule is **deny_server_rule** which is equivalent to the router's **deny ip any any** command.

Our VPN Concentrator filter is **filter_with_2_rules**, which is equivalent to the router's 101 access list; it uses **permit_server_rule** and **deny_server_rule** (in that order). It is assumed that clients can connect properly prior to adding filters; they receive their IP addresses from a pool on the VPN Concentrator.

Refer to PIX/ASA 7.x ASDM: Restrict the Network Access of Remote Access VPN Users in order to learn more about the scenario where the PIX/ASA 7.x block the access from the VPN users.

Prerequisites

Requirements

There are no specific requirements for this document.

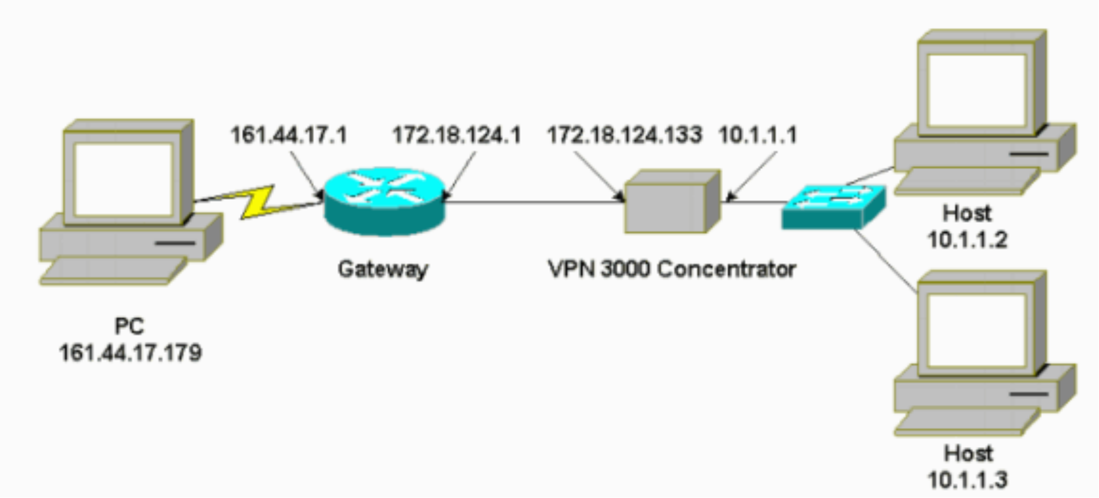
Components Used

The information in this document is based on Cisco VPN 3000 Concentrator version 2.5.2.D.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:



Conventions

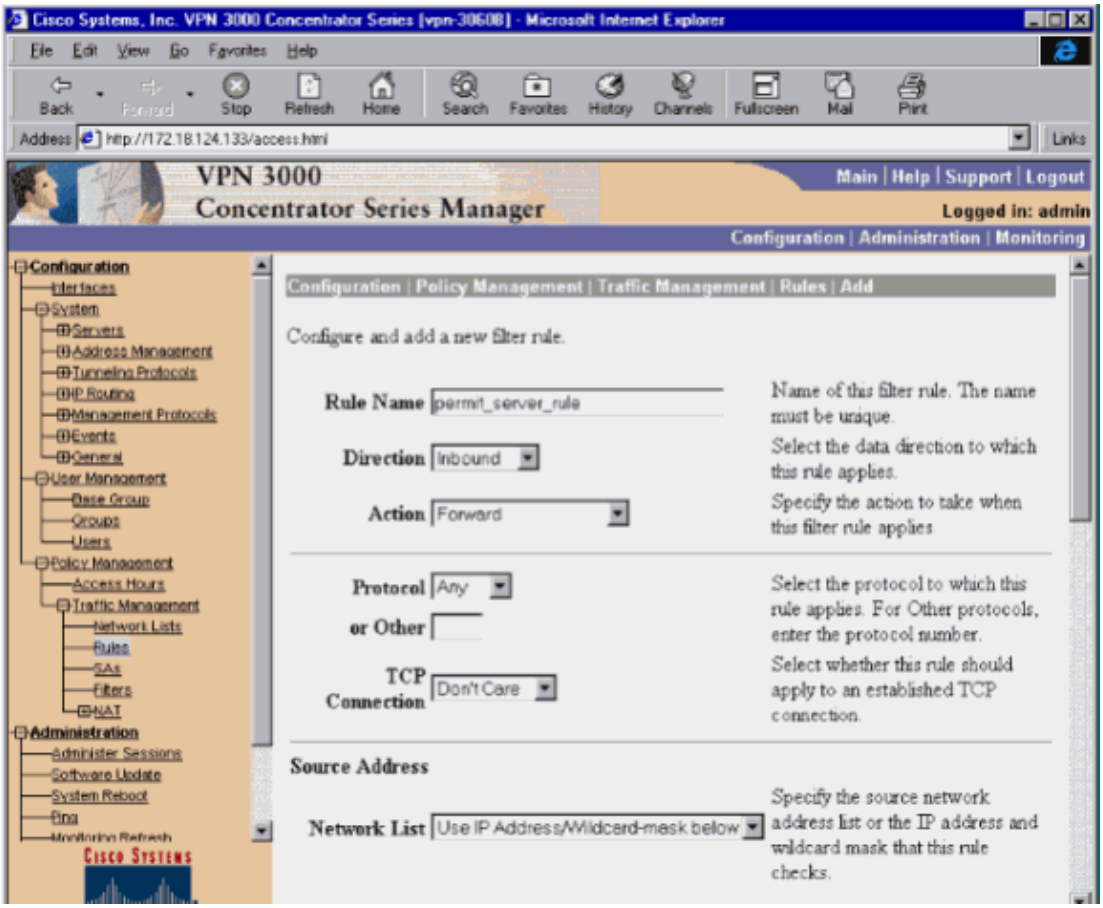
Refer to Cisco Technical Tips Conventions for more information on document conventions.

VPN 3000 Configuration

Complete these steps in order to configure the VPN 3000 Concentrator.

1. Choose **Configuration >Policy Management > Traffic Management > Rules > Add** and define the first VPN Concentrator rule called **permit_server_rule** with these settings:

    - Direction **Inbound**
    - Action **Forward**
    - Source Address **255.255.255.255**
    - Destination Address **10.1.1.2**
    - Wildcard Mask **0.0.0.0**



Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name: permit_server_rule — Name of this filter rule. The name must be unique.

Direction: Inbound — Select the data direction to which this rule applies.

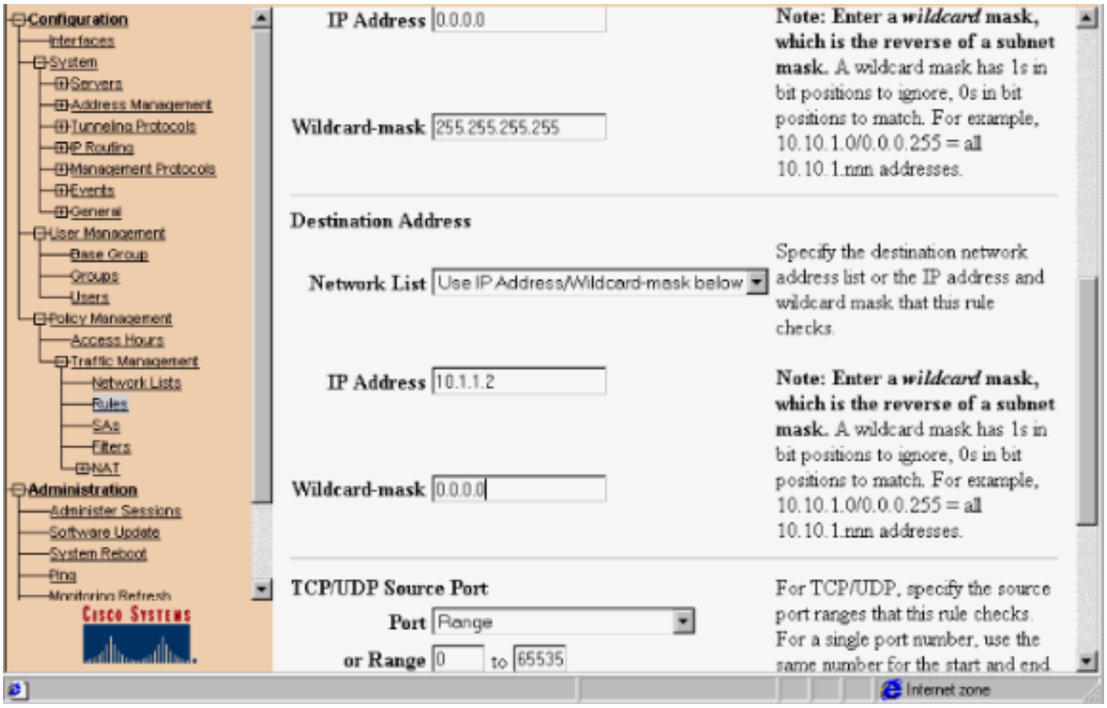
Action: Forward — Specify the action to take when this filter rule applies.

Protocol: Any — or Other: — Select the protocol to which this rule applies. For Other protocols, enter the protocol number.

TCP Connection: Don't Care — Select whether this rule should apply to an established TCP connection.

Source Address

Network List: Use IP Address/Wildcard-mask below — Specify the source network address list or the IP address and wildcard mask that this rule checks.



IP Address: 0.0.0.0

Wildcard-mask: 255.255.255.255

Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Destination Address

Network List: Use IP Address/Wildcard-mask below — Specify the destination network address list or the IP address and wildcard mask that this rule checks.

IP Address: 10.1.1.2

Wildcard-mask: 0.0.0.0

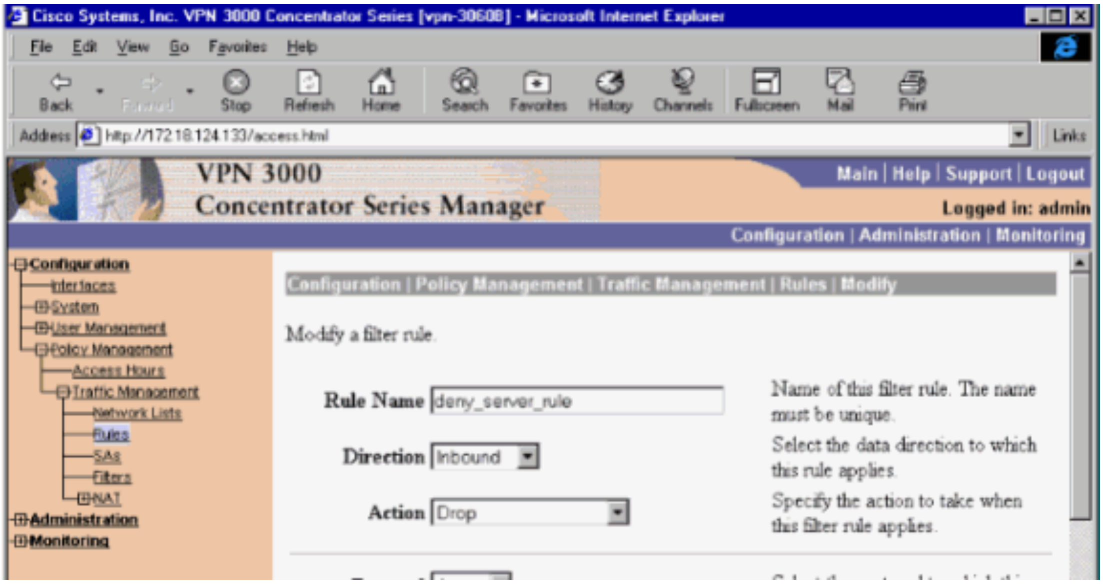
Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

TCP/UDP Source Port

Port: Range — or Range: 0 to 65535 — For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end

2. In the same area, define the second VPN Concentrator rule called **deny_server_rule** with these defaults:

- Direction **Inbound**
- Action **Drop**
- Source and Destination Addresses of anything (255.255.255.255):



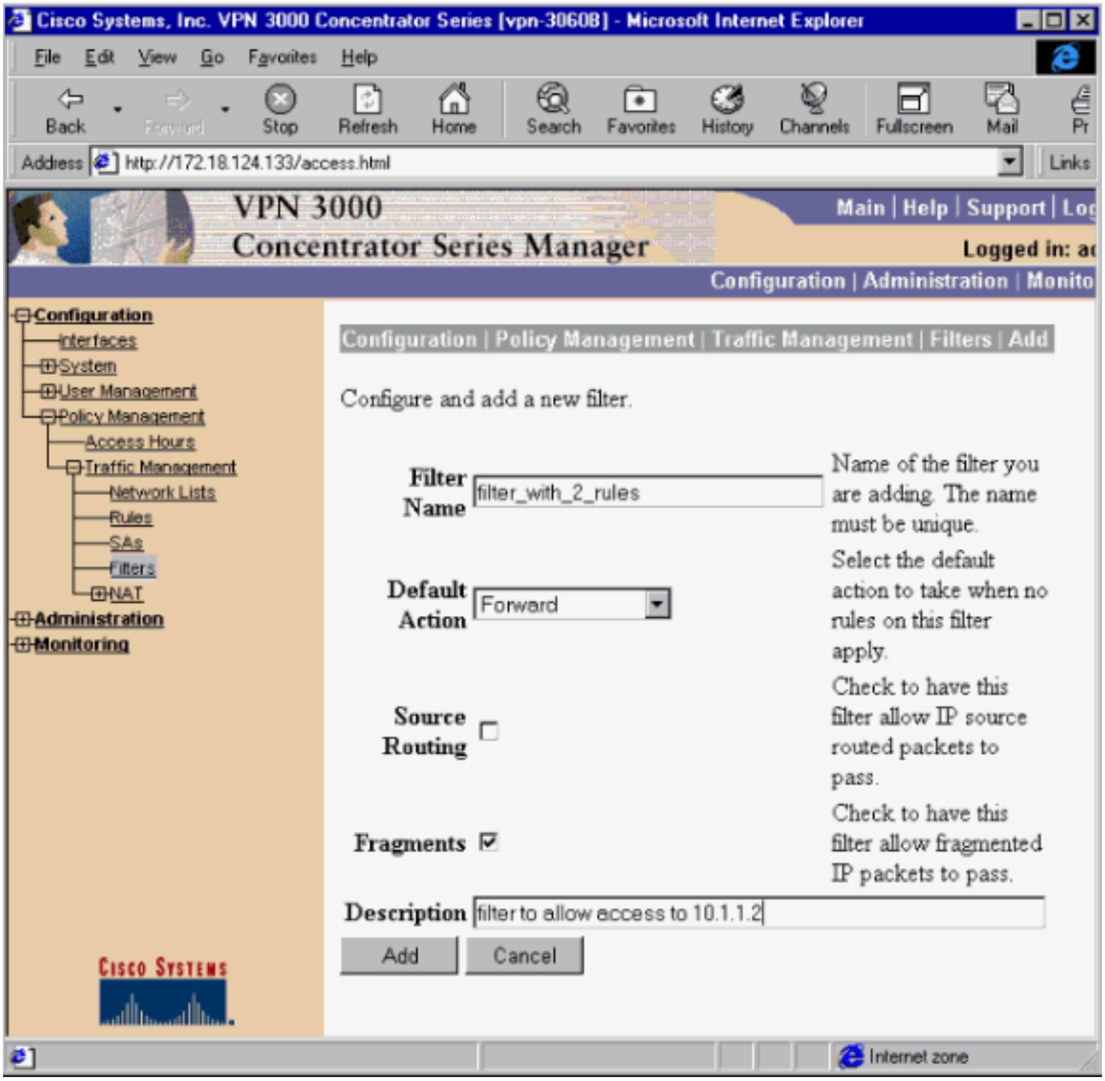
Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address http://172.18.124.133/access.html
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring

Configuration | Policy Management | Traffic Management | Rules | Modify

Modify a filter rule.

Rule Name	deny_server_rule	Name of this filter rule. The name must be unique.
Direction	Inbound	Select the data direction to which this rule applies.
Action	Drop	Specify the action to take when this filter rule applies.

3. Choose **Configuration > Policy Management > Traffic Management > Filters** and add your **filter_with_2_rules** filter.



Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Pr
Address http://172.18.124.133/access.html
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Log
Logged in: ad
Configuration | Administration | Monito
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Internet zone

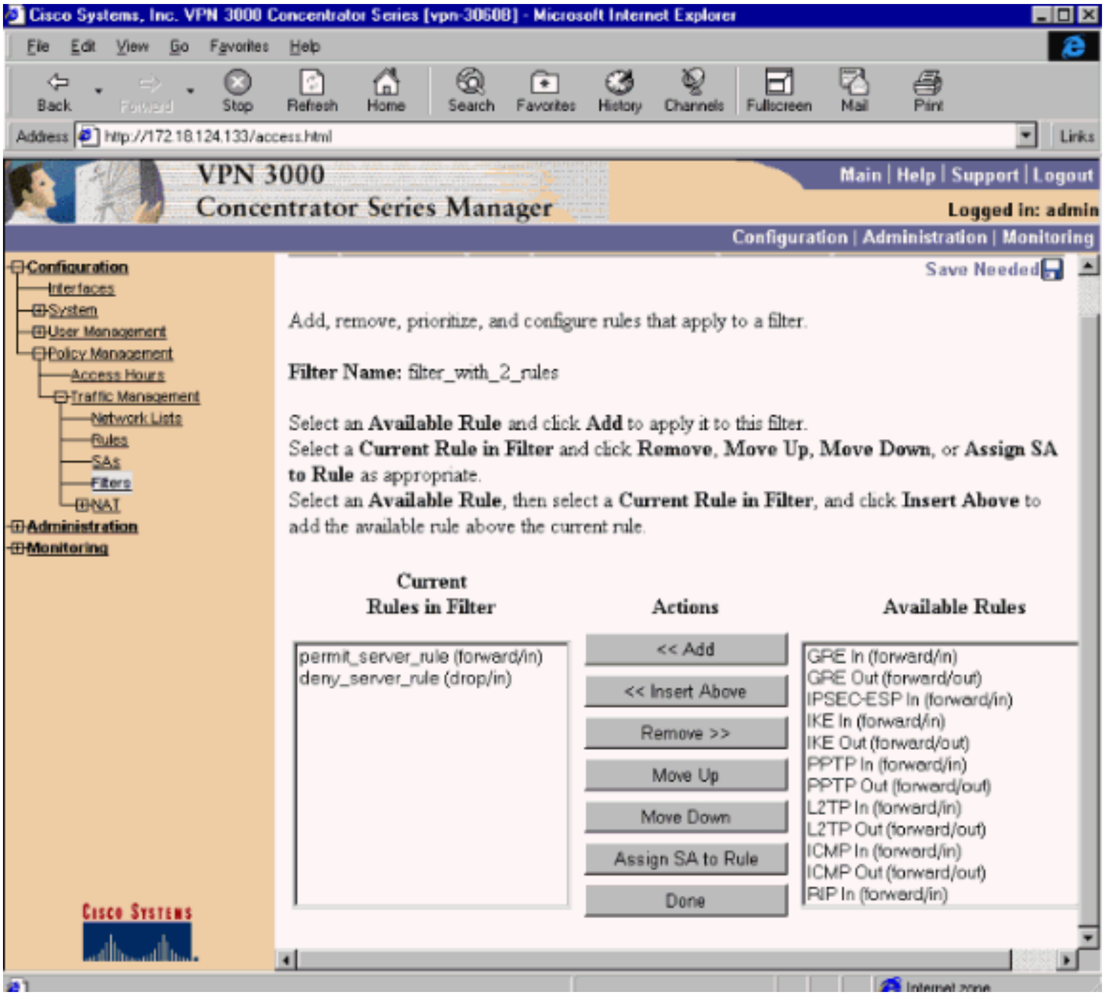
Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

Filter Name	filter_with_2_rules	Name of the filter you are adding. The name must be unique.
Default Action	Forward	Select the default action to take when no rules on this filter apply.
Source Routing	☐	Check to have this filter allow IP source routed packets to pass.
Fragments	☑	Check to have this filter allow fragmented IP packets to pass.
Description	filter to allow access to 10.1.1.2	

Add Cancel

4. Add the two rules to filter_with_2_rules:


Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30600] - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address http://172.18.124.133/access.html
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Save Needed
Internet zone

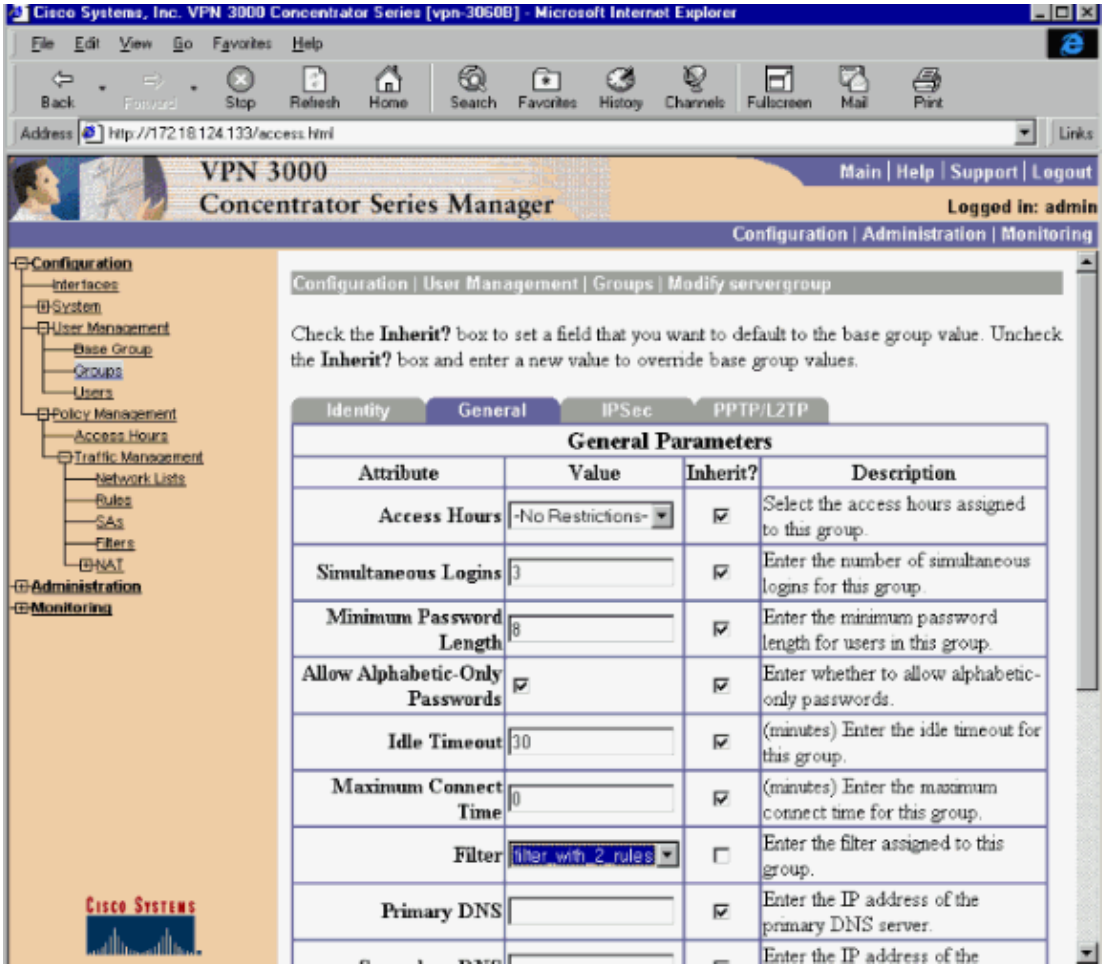
Add, remove, prioritize, and configure rules that apply to a filter.

Filter Name: filter_with_2_rules

Select an **Available Rule** and click **Add** to apply it to this filter.
Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.
Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter	Actions	Available Rules
permit_server_rule (forward/in) deny_server_rule (drop/in)	<< Add << Insert Above Remove >> Move Up Move Down Assign SA to Rule Done	GRE In (forward/in) GRE Out (forward/out) IPSEC-ESP In (forward/in) IKE In (forward/in) IKE Out (forward/out) PPTP In (forward/in) PPTP Out (forward/out) L2TP In (forward/in) L2TP Out (forward/out) ICMP In (forward/in) ICMP Out (forward/out) RIP In (forward/in)

5. Choose **Configuration > User Management > Groups** and apply the filter to the group:


Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address http://172.18.124.133/access.html
Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Identity
General
IPSec
PPTP/L2TP

Configuration | User Management | Groups | Modify servergroup

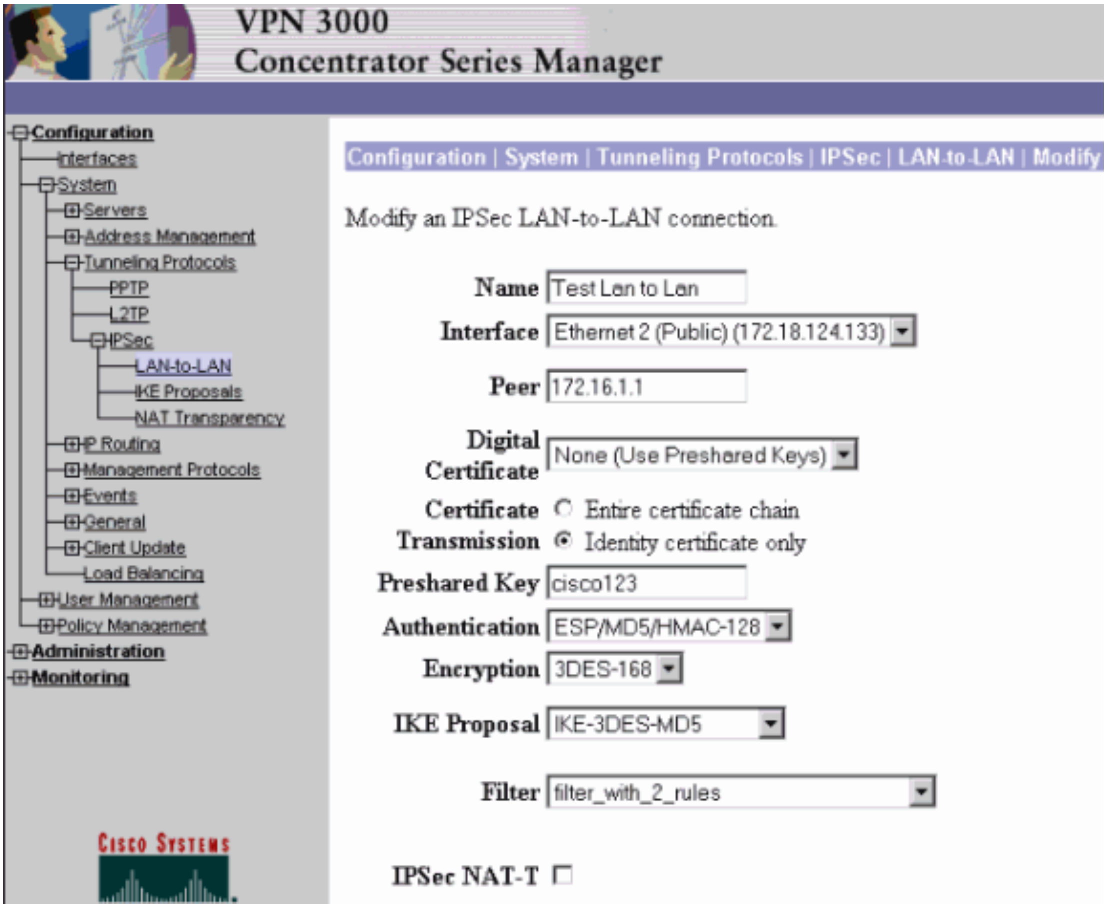
Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	filter_with_2_rules	□	Enter the filter assigned to this group.
Primary DNS		☑	Enter the IP address of the primary DNS server.
		□	Enter the IP address of the

Filters for a LAN−to−LAN VPN Tunnel

From VPN Concentrator code 3.6 and later, you can filter traffic for each LAN−to−LAN IPsec VPN tunnel. For example, if you build a LAN−to−LAN tunnel to another VPN Concentrator with the address 172.16.1.1, and want to permit host 10.1.1.2 access to the tunnel while you deny all other traffic, you can apply **filter_with_2_rules** when you choose **Configuration** > **System** > **Tunneling Protocols** > **IPSec** > **LAN−to−LAN** > **Modify** and select **filter_with_2_rules** under **Filter**.



Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name: Test Lan to Lan

Interface: Ethernet 2 (Public) (172.18.124.133)

Peer: 172.16.1.1

Digital Certificate: None (Use Preshared Keys)

Certificate Transmission: ○ Entire certificate chain ● Identity certificate only

Preshared Key: cisco123

Authentication: ESP/MD5/HMAC-128

Encryption: 3DES-168

IKE Proposal: IKE-3DES-MD5

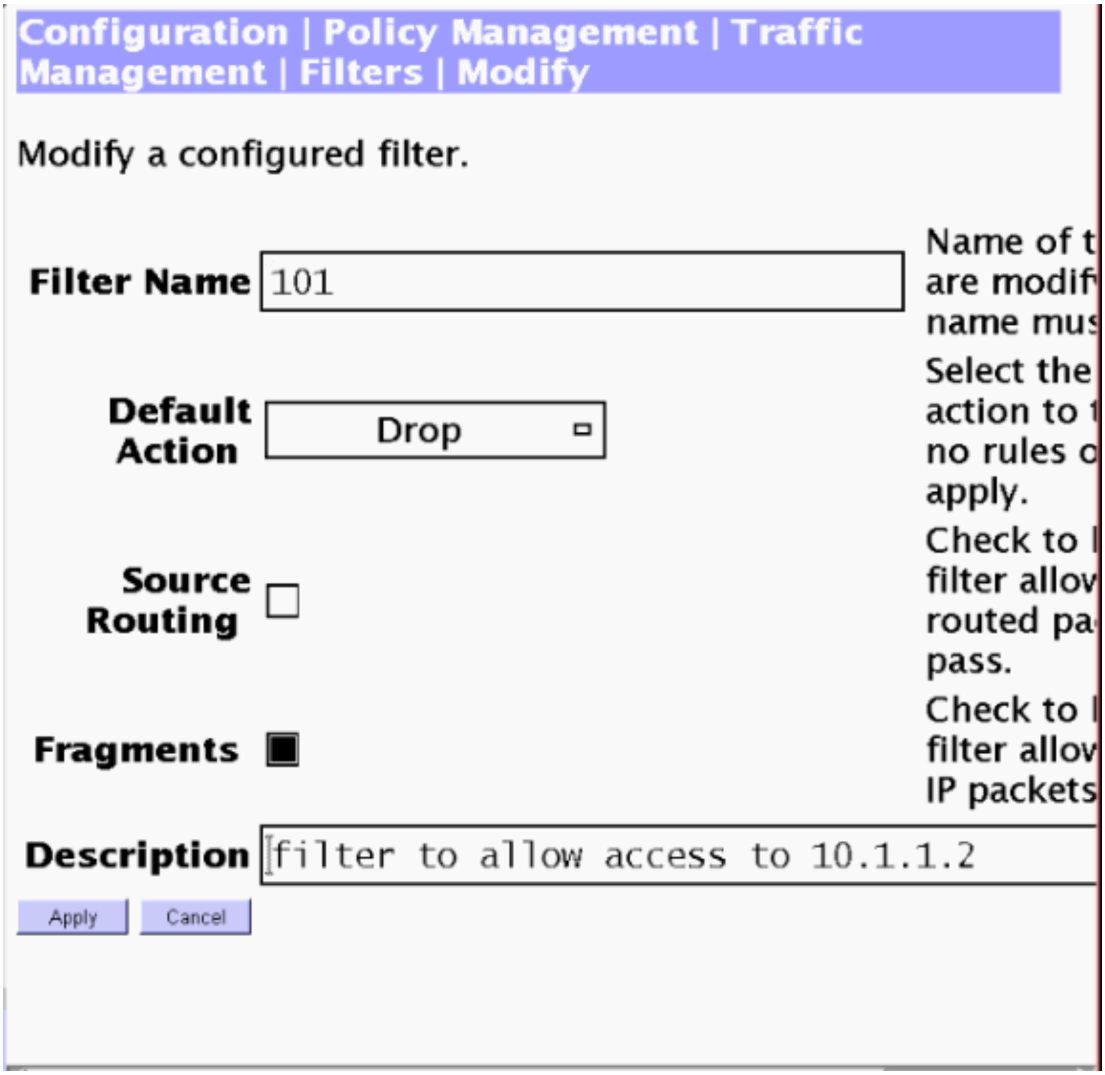
Filter: filter_with_2_rules

IPSec NAT-T: □

VPN 3000 Configuration − RADIUS Filter Assignment

It is also possible to define a filter in the VPN Concentrator and then pass down the filter number from a RADIUS server (in RADIUS terms, attribute 11 is Filter−id), so that when the user is authenticated on the RADIUS server, the Filter−id is associated with that connection. In this example, the assumption is that RADIUS authentication for VPN Concentrator users is already operational and only the Filter−id is to be added.

Define the filter on the VPN Concentrator as in the previous example:



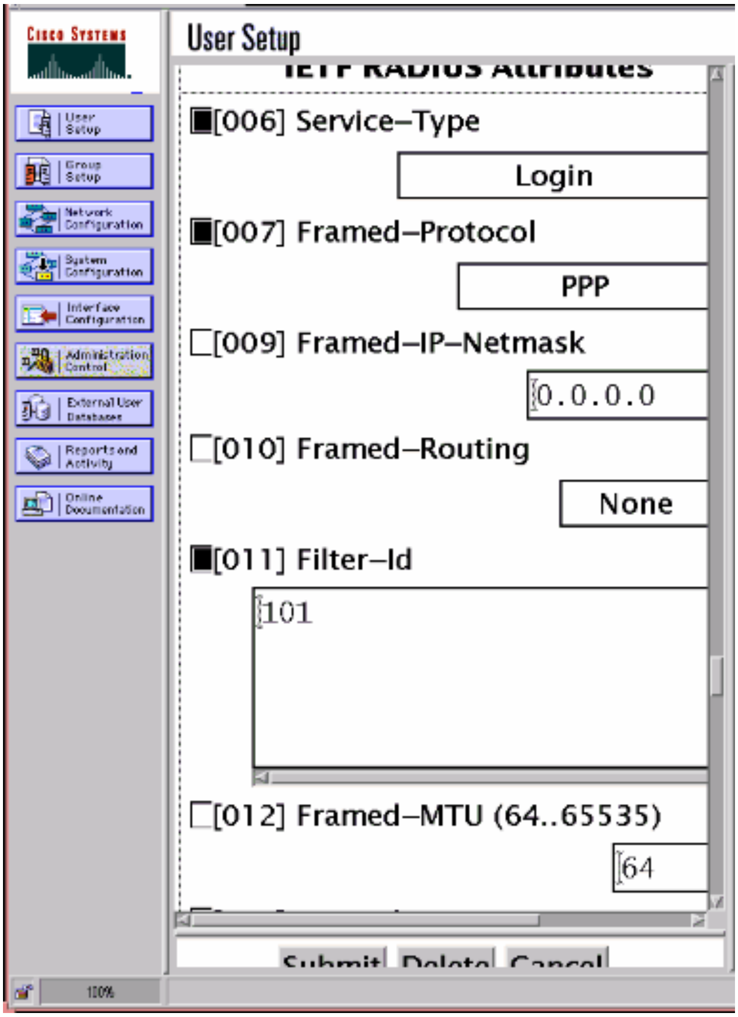
Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name	101	Name of t are modif name mus
Default Action	Drop	Select the action to t no rules o apply.
Source Routing	□	Check to l filter allov routed pa pass.
Fragments	■	Check to l filter allov IP packets
Description	filter to allow access to 10.1.1.2	

CSNT Server Configuration − RADIUS Filter Assignment

Configure attribute 11, Filter−id on the Cisco Secure NT server to be **101**:



User Setup

IETF RADIUS Attributes

■[006] Service−Type

Login

■[007] Framed−Protocol

PPP

□[009] Framed−IP−Netmask

0.0.0.0

□[010] Framed−Routing

None

■[011] Filter−Id

101

□[012] Framed−MTU (64..65535)

64

Debug − RADIUS Filter Assignment

If AUTHDECODE (1−13 Severity) is on in the VPN Concentrator, the log shows that the Cisco Secure NT server sends down access−list 101 in attribute 11 (0x0B):

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001     .v..............
0020: 0B053130 310806FF FFFFFF                   ..101......
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

For troubleshooting purposes only, you can turn on filter debugging when you choose **Configuration** > **System** > **Events** > **Classes** and add **FILTERDBG** class with **Severity to Log** = **13**. In the rules, change the Default action from Forward (or Drop) to **Forward and Log** (or Drop and Log). When the event log is retrieved at **Monitoring** > **Event Log**, it should show entries such as:

```
221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

```
222 12/21/2000 14:20:18.690 SEV=9 FILTERDBG/1 RPT=63
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

Related Information

- **IPsec Negotiation/IKE Protocols**
- **VPN 3000 Concentrator Frequently Asked Questions**
- **RADIUS Support**
- **Cisco VPN 3000 Concentrator Support**
- **Cisco VPN 3000 Client Support**
- **Cisco Secure ACS for Windows Support**
- **Request for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 07, 2007 Document ID: 13834